NPS-97-03-002

NAVAL POSTGRADUATE SCHOOL
Monterey, California

ASOCC Demonstration – System Evaluation for NCIS Use

Gordon Schacher and Shelley Gallup
Wayne E. Meyer Institute of Systems Engineering

28 March 2003

Approved for public release; distribution is unlimited.

Prepared for: Naval Criminal Investigative Service

20030508 093

This Page Intentionally left Blank

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

RADM David R. Ellison, USN
Superintendent

Richard Elster
Provost

This report was prepared for: Naval Criminal Investigative Service

Reproduction of all or part of this report is authorized.

This report was prepared by: Wayne E. Meyer Institute of Systems Engineering

Gordon Schacher
Professor Emeritus

Shelley Gallup
Research Associate Professor

Reviewed by:

Phil DePoy, Director
Wayne E. Meyer Institute
of Systems Engineering

Released by:

D. W. Netzer
Associate Provost and
Dean of Research

REPORT DOCUMENTATION PAGE

Form approved

OMB No 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 28 Feb 03	3. REPORT TYPE AND DATES COVERED Research

4. TITLE AND SUBTITLE
ASOCC Demonstration - System Evaluation for NCIS use

5. FUNDING
MIPR No. N6328503MPERF02

6. AUTHOR(S)
Gordon Schacher and Shelley Gallup

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Wayne E. Meyer Institute of Systems Engineering
Naval Postgraduate School
777 Dyer Rd., Room 100D, Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Naval Criminal Investigative Service
716 Sicard St, SE
Washington Navy Yard, Bldg 111. Washington, DC 20388

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words.)

The Area Security Operations Command and Control system is being tested for Homeland Security applications through an ACTD. A multi-agency, nation-wide, demonstration of the system has been conducted. This report presents an evaluation of the system for Naval Criminal Investigative Service use using results from the demonstration.

14. SUBJECT TERMS
Anti-Terrorism, Force Protection, Information Systems, Homeland Security

15. NUMBER OF PAGES 32

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

NSN 7540-01-280-5800

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18

ASOCC Demonstration – System Evaluation for NCIS Use

Gordon Schacher and Shelley Gallup
Wayne E. Meyer Institute of Systems Engineering
Naval Postgraduate School

TABLE OF CONTENTS

	Page
I. Executive Summary	1
II. Background	2
III. NCIS Organizations and Pertinent Tasks	3
IV. HLS ACTD Purpose and Requirements	4
V. ASOCC Capabilities	5
VI. Demonstration Structure	7
VII. Data and Information Capture	9
VIII. Results	10
IX. Wider NCIS Considerations	13
Appendices	
A-1. Completed ASOCC Evaluation Surveys	15
A-2. Master Script Introduction	21
A-3. Network Based Information System Requirements	26
Distribution List	31

This Page Intentionally left Blank

I. Executive Summary

Results Quality: The activity from which this information was derived was a demonstration, not an experiment. Thus, there were limited opportunities to obtain objective data. Regardless, participation by experienced NCIS personnel enabled obtaining valuable insights into use of ASOCC by NCIS.

Only MTAC actually participated in the demonstration. The NCIS Field Officer was an observer and not able to do any hands-on work with the system.

Human Factors: Use of the system is intuitive for those who have had experience with web-based systems. Training would be needed to realize its full potential, but this should not require much time or effort.

It is expected that up to three people would be needed to man the system during an emergency, depending on the extent to which MTAC wanted to participate in real-time activities during a terrorist event.

Regardless of whether or not a person can keep up with ASOCC information, it will take considerable analysis skill to interpret, correlate, assess, and provide conclusions from the information. Because the information is more diverse than is currently dealt with,

additional analysis training and experience may be needed to utilize fully the system. For example, knowledge of law enforcement and emergency procedures will be needed.

Information Content: The information presented is quite complete. This very completeness can lead to information overload and an inability to find needed information. There is a problem with all information being is treated as equal. This means that an operator has to sift through a significant quantity of information before reaching a critical item.

Presentation that segments by user, priority, and criticality is needed.

A means to navigate directly from an alert to pertinent information is needed.

Collaboration: MTAC collaborates with other members of the intelligence community. Current methods are adequate during normal business but can be slow, or even interrupted or overloaded, during a crisis situation.

ASOCC provides improved collaboration opportunities, redundancy, easy multi-unit collaboration, and perhaps improved timeliness.

Integration of Law Enforcement into MTAC products is a current priority. This system provides a means for doing that rather easily.

Coverage: MTAC has the responsibility to reach all Navy units and Field Officers.

ASOCC will be available only at large installations that have high data rates available.

Thus, this system cannot replace existing means for information exchange because will not be in place at all units.

Opportunities: ASOCC opens up new opportunities for NCIS.

Closer, more rapid, collaboration with other organizations.

Real-time communication with new organizations, especially local agencies.

Maintaining real-time situation awareness during a crisis event.

Making substantial use of these capabilities in order for it to be worth the effort would require an expansion of NCIS's activities.

Recommendations: Based on the information reported here, it is not possible to provide a definitive recommendation concerning ASOCC adoption. More information is needed, preferably provided from a more complete operational test of the system. However, for other considerations, ASOCC will be adopted by the Navy in a manner not yet defined. Exactly how and how extensively this will be done are not known. Thus:

The immediate question becomes how to implement ASOCC for MTAC and other NCIS operations within the reality of DoD use for HLS.

The following recommendations are based on this situation.

Important considerations are:

One information management and distribution system cannot be expected to meet all NCIS requirements.

Whether NCIS, including MTAC, will participate more closely with law enforcement and response organizations in crisis planning and consequence management.

Many units and organizations with which MTAC exchanges information have limited bandwidth and will not have ASOCC available.

A comprehensive review is needed of NCIS operations, both current and projected, and the information system(s) needed to support these operations. This would entail looking at current and possible future CONOPS and TTPs. Consideration should be given to availability and use of the following systems:

Navy, DOD, and HLS ASOCC implementation.

NCIS established requirements for a web-based information system (TATIPS).

Adoption of other systems within DoD (e.g. JRAMP by EUCOM).

NCIS planned knowledge management system supporting area information drawers.

IWCCS being brought ashore from carrier battle groups.

RASP use by NCIS field agents.

II. Background

The Area Security Operations Command and Control (ASOCC) system was developed for Pacific Command (PACOM) to coordinate operations within their Area of Responsibility (AOR). PACOM has a somewhat unique set of needs because of the large size of their AOR and the wide diversity of their operations, including humanitarian assistance and disaster relief. A coalition

version of ASOCC was also developed to extend the system to coalition partners and also to non-government organizations that participate in non-military operations.

With emergence of the need for Homeland Security (HLS) operations it was natural to investigate extending ASOCC into this arena. Thus, an Advanced Concepts Technology Demonstration (ACTD) for Homeland Security Command and Control (HLS C2 ACTD) was instituted. The mission of the ACTD is to "identify, demonstrate and transition mature and maturing information technologies and CONOPS that increase DoD efficiency and effectiveness in Homeland Security missions."

The purpose of the research reported here is to determine if and how ASOCC capabilities can be applied to assist the Naval Criminal Investigation Service (NCIS) in meeting its mission. The principal focus is on use within the NCIS Multi-Threat Alert Center (MTAC). Comments on use for the wider NCIS mission and tasks are also provided in this report.

ASOCC is designed to be a situational awareness tool for use during emergency situations. It provides information sharing for the large number of organizations involved in a crisis activity and enables coordination amongst them. It is web-based, containing means for

displaying information from a variety of sources,
real-time collaboration, and
providing paths for assessment information exchange.

It requires a dedicated server and a large information pipeline for image transmission.

Currently proposed is to place ASOCC servers at major DoD shore installations and at various Emergency Operating Centers to support Homeland Security. It is not expected that the system will be available at small installations or on ships.

III. NCIS Organizations and Pertinent Tasks

We are concerned here with only those NCIS organizations that could possibly use ASOCC to help accomplish their missions. The organization descriptions here are quite incomplete, providing only information to indicate how the system might contribute. ASOCC can provide support for the following processes:

intelligence information input,
assessment information output,
resource visibility and coordination,
shared analysis (within NCIS and in collaboration with other agencies) , and
incident situational awareness.

The information can be used for:

an alternate or additional path for current information processes,
crisis event situation awareness and management,
post-crisis analysis,
daily activities.

The organizations within NCIS that map onto these processes and situations are:

Multi-Threat Alert Center.
Counter-Terrorism Directorate.
Law Enforcement and Physical Security Programs.
Criminal Investigations Directorate.
Computer Investigations and Operations Directorate.
Field agent activities.

Each of these organizations ingests various types of information, assesses that information, and produces and widely disseminates products. Examples of the many products are:

MTAC - Threat Assessments, Blue Darts, SARs
LEPS - Vulnerability Assessments, Physical Security Assessments
CTD - Lessons Learned, SARs, SIs, Best Practice, JTTF Coordination
CID - Criminal Alerts, Trends, Crime Scene Response

In addition to the above organizations and missions, NCIS is in the process of developing and implementing a comprehensive Knowledge Management system. It will contribute to fusing various types of information and placing it into regional "drawers". Productive interaction between ASOCC archiving and this Knowledge Management system may be possible. This possibility is not examined in this report.

At all levels the NCIS mission is to ingest, analyze, and disseminate information. NCIS already has available information paths and analysis processes. Every activity mentioned above is currently supported. The overriding questions with respect to ASOCC are:

Can it improve quality and/or speed of existing processes?
Can it enable useful collaboration that does not currently exist?
Can it enable new processes that would be of benefit to NCIS and the Navy?

With regard to the last question, there is currently little NCIS participation in real-time response, especially consequence management. Should there be?

IV. HLS ACTD Purpose and Requirements

As was stated above, the mission of the HLS ACTD is to "identify, demonstrate and transition mature and maturing information technologies and CONOPS that increase DoD efficiency and effectiveness in Homeland Security missions." To this end, CONOPS will address anti- and counter-terrorism, including:

Integration of intelligence, law enforcement, and scene of action information.
All-source assessments and alerts in support of federal, state, and local efforts.
DoD C2 within and across multiple missions and multiple chains of command.
DoD coordination with civil authorities at all levels.
Coordination of DoD and other federal HLS activities in military base areas.

Technology to support these activities is to include:

Information management.

Complex visualization.
Collaboration.
Alerting.
Command and Control (C2).
Reporting and archiving.

System requirements to meet these goals are spelled out in a set of Northern Command (NORTHCOM) requirements for a HLS Common Operational Picture (COP). The following is an abbreviated version of these requirements.

With regard to organizations deployed within the NORTHCOM AOR, the system must allow participation by and visibility of:

All land, air, maritime, and Military Assistance to Civilian Authorities (MACA).
FEMA deployed organizations.
Other Federal Departments.
Garrison and deployed WMC CSTs.
Local, state, and federal law enforcement organizations of interest.
Etc.

It must contain the following types of information:

Display of all near/entering maritime tracks.
COP from combatant and functional (STRATCOM, TRANSCOM, etc.) commands.
USCG vessel and cargo/manning.
Display WMD effects, simulations, and predictions.
Pull in other databases and overlays, NIMA, PACE, ArcIMS databases.
Current Consequence Management situation.
Resource use and availability.
Etc.

It must have collaboration capabilities, through chat, whiteboard, shared files, etc. to:

Edit, modify, create, delete tracks.
Direct and integrated AMICC and FAA feeds.
Full intelligence query and display from MIDB and other sources.
Creation and broadcast of overlays.
Overlays of all control measures at the local, state, and federal levels.
COP-based information from text-based INTSUMs, SITREPs, etc.
Etc.

V. ASOCC Capabilities

ASOCC is a toolkit providing means for exchanging text, graphics, pictures, and video, and for collaboration. It has extensive archiving for post-event playback and analysis. The following description of ASOCC capabilities is not complete in either toolkit components or descriptions. It is presented only to give a flavor of what the system contains. Those wishing complete descriptions can contact Jim Sherlock, SAIC, at james.c.sherlock@saic.com.

Hardware and Operating System:
Each operational node requires a PC with Pentium IV, 1.5 MHz, 512K memory, and 60 MB hard drive. The operating system can be either NT 4.0 or 2000, depending on local requirements. Three flat panel screens are needed, at least 17 inch, 3072 x 768. A baseline Microsoft suite is needed, including Office, Outlook, and Internet Explorer.

The normal display configuration is to use the left screen for information push, the middle for situational awareness and the right for information pull. The actual configuration is a matter of taste and multi-screen display for a single application is possible.

eX-Panel:
The eX-Panel provides Java/XML/XSLT based views for real-time logging, alerting, and event visualization capabilities. It is configured to provide:

General information and alerts: general advisories; alerts for threats, emergencies, situation conditions; checklists linked to alerts; event search to support analysis.

Actionable events: pop-up and audio alarms; event tab precedence showing actions taking place, actions required, action status; checklists; event record content.

Local situation visualization: visualization summary of conditions, alerts at locations, geo-referenced events displayed on maps.

Force protection condition management: top-down directed actions, bottom-up conditions reporting, SITREPS.

Knowledge Board: (KB)
KB is a data fusion tool that provides a web-based, distributed information view port. It facilitates the display and review of information from many heterogeneous data sources. KB scripting provides:

Portal management of related views based on web and enterprise content.
Amplifying information for daily operations.
Tailored views and source selection relevant to the problem at hand.

Java Video Imagery Exploitation: (JIVE)
JIVE provides access to tactical imagery:

Geo-registered tactical imagery resources on intelligence community servers.
Viewing and manipulation of multiple formats with overlay and text.
Live and queued video streams from UAVs and sensors.

It is DCTS enabled for collaborative planning.

eXtensible Information System: (XIS)
XIS is an open standards information management tool used to bring relevant information from disparate domains and formats together into integrated views.

Geo-spatial capability can support input from CADRG, DTED, Arc IMS, Arc View Shape files, JPEG, GIF, etc.

Can fuse additional data layers on top of the underlying maps and images, e.g. force data, GCCS track data, and MIL Standard 2525B symbols.

XIS scripting can be used in crisis response and situational awareness modes:

Crisis response mode:

cued by an event symbol on a map
build a geo-spatial picture from varied data sources
drag in track or force data
share through NetMeeting/DCTS

Situational awareness mode, can monitor the fused operational picture:

tracks, forces, images

Deployment Visualization Toolkit: (DVT)
DVT provides read-only access to JOPES database and GCCS Track Database Manager. It uses XIS to display force deployment data. It provides:

Tracking of allocated forces, including unit ID, organization structure, location, and deployment status.

Defense Collaborative Tool Suite: (DCTS)
DCTS provides H323/T120 standards based collaboration services using NetMeeting and Internet Explorer with the CUseeMe multi-point server. Collaboration is enabled with any user having a Microsoft operating system and Internet access. Audio, Video, document transfer, Whiteboard, Chat, and application sharing are all provided.

The system can be used in either synchronous or asynchronous mode. It can be used as a repository for pre-staged maps and imagery for use with XIS.

VI. Demonstration Structure

The purpose of the event was to demonstrate:

ASOCC technology capabilities and
Concepts of Operations (CONOPS)

for DoD participation and collaboration with other organizations in an HLS scenario. State, local, and other federal agencies participated, but the principal focus was on DoD CONOPS. It was hoped that demonstrating the system broadly would lead to adoption of ASOCC by other organizations or to their participation in further development of requirements and creation of a HLS COP and collaboration system.

The demonstration was divided into five phases:

Indications and warnings.
Deterrence, prevention, and protection.
Attack.
Crisis Action Planning.
Crisis and Consequence Management.

Terrorist attacks were at and around Navy and Marine facilities in the continental U.S.:

A ship-born nuclear attack approaching from outside the continent.
Direct use of chemical agents against a base.
Destruction of civilian facilities resulting in the release of hazardous agents.
Destruction of transportation capabilities around bases.
Small boat attack on a Navy carrier.

Attacks and threats were at:

Attacks	Threats
Tidewater Virginia.	Puget Sound
San Diego area.	New York harbor
Batten Rouge area.	

Participants in the demonstration were:

NORTHCOM	JFCOM	LANTFLT	PACFLT
MARFORPAC	CNO Cmd Cntr	CMC Cmd Cntr	USCG
DIA/JITF/CT	USCG	NCIS	JFHQ HLS
JTF-CS	NIMA	DTRA	DISA
FBI - NIPC	FEMA	ATF	Marshal Service
Navy MIDLANT	Navy SOWEST	NAS North Is	NCAS Mirmar
Camp Pendleton	NAS Norfolk	CG LANTAREA	

Louisiana State	Virginia State	NY City EOC
EOC	EOC	WA State EOC
National Guard CST	DCO	
State Police	National Guard CST	
Port Authority	Port Authority	
	City of Norfolk	
	City of Chesapeake	

The demonstration had a two-day practice on 3-4 Dec then was carried out on 9-10 Dec. Execution of the large number of actions, all the way from Indications and Warnings to Consequence Management, over a two-day period required time compaction and rigid control. Demonstration personnel at each node assisted players and, if needed, performed their functions. They were responsible for insuring the demonstration schedule was followed.

Both played and stipulated events were used. Played meant that an activity person, or sometimes demonstration personnel, provided input of information into the system. Stipulated meant that the action was designated in the script but not performed. All physical actions were stipulated.

The purpose of the demonstration was to show how ASOCC capabilities could be used for homeland defense but not to test how well the system would support such activities. Because of this demonstration format, information that was input to the system was prepared before the event. Thus, there was no

accessing of information,
information analysis, and

subsequent decision-making.
This was appropriate for this stage in ACTD development but limited evaluation of the system.

VII. Data and Information Capture

General Comments
Operational experiments normally provide both data and information. Data is obtained by recording events, both by electronic and human means. Subjective information is obtained from operator opinions about system, process, and human performance, and the adequacy of human-machine interactions. The demonstration vice experiment format had an impact on data and information capture, most important that opportunities for data capture were not present.

There were two major impacts on obtaining needed information.

1. Pre-scripting of demonstration input and output information means no results could be gathered on efficiency or lengths of time for:
   information acquisition,
   comprehension,
   assessment, and
   information output.

2. Pre-scripting of event physical actions, including their impacts, means that results could not be obtained on
   improved situation awareness,
   information impacts on human decision and actions, and
   information impacts on organization functions.

Information Capture
This project's goals were to:

1. Compare performance of MTAC functions using ASOCC and existing means.

2. Determine if ASOCC situational awareness information improves the quality of MTAC assessments and subsequent information provided to Navy units.

To meet these goals, the initial test plan focused on ASOCC use by MTAC to
obtain information from NCIS field agents,
obtain information from other intelligence providers,
provide information to Navy units,
collaborate with other activities during a crisis event, and
conduct daily activities.

The parameters to be determined are
time required to perform a function,
effort required to perform a function, and
manpower required to staff the operation.

As a result of these data and information acquisition restrictions noted above, there is an inability to present unambiguous results with respect to system utilization by NCIS. This does not render the ASOCC demonstration useless for this purpose, rather the results reported here are subjective and preliminary. As examples, participants can judge whether information exchange will be speeded compared to current methods used. Also, they can judge whether ASOCC opens possibilities for providing services not currently available, one goal of this project. Such judgments are of value but not definitive because no test of time-to-completion or new services was actually made. Regardless, such opinions are of high value. They are from people who have considerable experience in performing their various tasks, and apply this experience to judge how ASOCC will aid, or hinder, their performance.

Effort required to perform functions is also subjective information from MTAC operator's opinions. This information is somewhat compromised because of the small amount of training operators receive on ASOCC and the short time allowed for the experiment, compared to familiarity with current means.

A significant parameter is the numbers of units outside MTAC that are able to access information MTAC provides and how quickly. There were no plans to determine this parameter and it should be the object of subsequent studies.

Because of the demonstration format, only limited information could be obtained for manpower requirements for ASOCC use. MTAC staffing requirements are needed for

current activities (baseline),
activities during a crisis using conventional means,
use of ASOCC for current activities,
continuous ASOCC monitoring, and
use of ASOCC during a crisis.

Determination of these staffing requirements should be undertaken.

An NCIS field agent was a demonstration observer but not an active participant. The information provided is with regard to possible uses of the system in the field based on a judgment of what a fully functional and staffed system could provide.

VIII. Results

Initial planning for demonstration analysis was to determine four basic measures:

time required to perform a function,
quality of job performance,
effort required to perform a function, and
personnel requirements,

and to compare these parameters for performing the functions with and without ASOCC.

Secondary considerations were to determine:

Could ASOCC replace existing information exchange means?
Can the system enable new functions that would be of value to NCIS/MTAC?
Is broad-based situational awareness information of value to fulfilling NCIS's mission?

One NPS observer was at MTAC and one at Norfolk during the demonstration. One MTAC operator and one NCIS Field Agent completed questionnaires that were designed to obtain the above information. Completed questionnaires are presented in Appendix 3. The following results are obtained from analysis of the information provided by these four sources.

As noted previously in this report, objective measures of time required to perform tasks and output quality could not be obtained. Thus, results that deal with these topics are participant opinions based on their experience and limited observations during the demonstration.

Participant Survey Results Summary

A summary of answers to direct questions is presented first (see Appendix 1 for the raw data) followed by a summary of comments for each section.

A. Effort to perform a task with ASOCC compared to existing means:
Ease and speed of information processes was judged to be better to much better. An exception was MTAC perception that information dissemination would be harder. This is interpreted as being due to information paths to reach small units such as ships not being available.

B. ASOCC system performance:
System navigation was favorably judged. It was recognized that training would be needed for efficient use, but that the amount would small.

System Design was favorably judged, with *visual layout* being higher rated than *information comprehension*. Three screens allowed much information to be presented, but all three were not often used at the same time. Operators were allowed to configure screens as they pleased and they did not have sufficient experience with the system to arrive at a configuration that met their particular desires. This is either an experience or training issue, or both. System design appears to be flexible enough to accommodate individual tastes.

The suggestion was made that, during a real *crisis management* situation, two or three people would be needed to cover adequately the information. A suggested configuration is to have two operators, each with a screen, and the third screen devoted to imagery of ongoing events.

A *design strength* is the ability to simultaneously view information while conducting Chat or other collaboration means. Also, simultaneous collaboration with several entities is a plus.

Information content is judged to be *complete*.

C. Information overload:
Information overload appears to be a problem. The most significant difficulty is keeping track of which information is critical and requires decision-maker attention. Corrective suggestions are:

Improved alerting to identify critical information.
Alerting that identifies input source, criticality, and tasking.
A system method that allows going directly from an alert to pertinent information.
Use a watch manager, deciding which information to have accessed, and assigning tasks.

D. Collaboration:
Collaboration tools were judged very favorably. One of the main activities of MTAC is information sharing and collaboration throughout the intelligence community and this system allows that to be done effectively.

The system allows effective collaboration when other media are tied up or unavailable.

E. New capabilities:
Information here was mixed because of the different perspectives of a MTAC watch-stander and a Field Agent. Reliable information content for this question is too low to derive results. There is the sense that information provided by this system could be more timely, representing an opportunity in the field and for decision-makers.

F. Manpower:
MTAC need for additional manpower for this purpose can only be answered in the affirmative because of the current MTAC personnel shortage to perform current tasks. The demonstration did not provide information indicating there would be sufficient efficiencies due to ASOCC use for that factor, in itself, to warrant its use.

There is, as yet, no understanding of manpower and training requirements for ASOCC use for current tasks, even less so for possible new tasks.

G. Situation awareness:
Enhanced situation awareness could lead to information updates that would result in production of SARs, SPOT reports, and/or BLUE Darts.

H. Special interest topics:

The following are general comments made by the MTAC watch-stander and the Field Agent who observed the demonstration in Norfolk. They are presented unedited and without comment.

<u>MTAC Watch-Stander Comments</u>
1) Once this system is fully operational, it would enhance the MTAC's capabilities. But, until this system the NCIS field offices and resident offices, ASOCC will not be very useful, other than monitoring for Law Enforcement information on the UNCLASSIFIED (NIPRNET).

2) The Collaboration tool was very interesting. I can see this enhancing the MTAC capabilities when more intel agencies join the system.

3) Disseminating information that the MTAC would put out via ASOCC does not reach the required assets that MTAC needs to reach (ie. naval ships) since they only have a very limited bandwidth to receive information.

4) Overall, I thought the experience with ASOCC very informative. The system possess the capability to enhance the situational awareness of the MTAC.

Field Operator Comments

1) The law enforcement personnel (to include Naval Criminal Investigative Service) working the system need to have a strong analytical background combined with strong computer/technical skills. The ideal candidate to operate is a full-time analyst (ideally two analysts at the field office level) from the field office or headquarters level who has:

- Strong working knowledge of the field office's physical area of responsibility (AOR)
- Strong working knowledge of state and local LE / Fire Emergency agencies in the AOR
- 2-4 years experience as a dispatcher at the field office or other LE/emergency agency
- Technical skills to maintain operations in case of minor glitches, power outages, emergency situations

2) Ideally three special agents and one supervisory special agent assigned to the field office Crisis Response Team (or Major Crime Response Team) should receive training in the field aspects of using these collaborative tools in order to have at least one agent in the office at all times who can work the PDA to Chat / White Board system. Those agents should first receive training in areas of:

- Basic WMD Crisis Mgt / Disaster response training (field agents)
- Basic Incident Command System (supervisor) training
- Strong working knowledge of the ASOCC system to include exercise and real world experience in utilizing the system (in case of limited number of analysts and agents)

IX. Wider NCIS Considerations

As has been noted above, this project has obtained direct information only about ASOCC use by MTAC and indirect observations about possible Field Agent use. Before adequate planning for use of the system can be made, wider use within NCIS should be considered.

First it must be recognized that this system is designed as an information exchange and collaboration medium for real-time crisis planning, events during a terrorist attack, and consequence management. It has an archival capacity, but only to store and replay event information. It is not a candidate for a knowledge management system to support NCIS analytic functions, such as that being designed for NCIS by SPAWAR.

Whether ASOCC, or such a system, is both useful and cost effective for NCIS can be addressed through a set of questions.

a. Is real-time, event, situation awareness information needed for any NCIS operations?
b. Is improved collaboration needed for existing purposes?

c. Are new types of collaboration needed in the current environment?
d. Are alternate paths needed for current operations for either speed or redundancy?
e. If ASOCC is adopted by other organizations, will NCIS use be necessary?
f. Are there needed NCIS functions not currently being done which an
g. ASOCC-like system would enable?
h. Are there current NCIS functions needing improvement that could be helped by new information and collaboration systems?
i. Are other information systems coming which may be imposed, can provide ASOCC-like capabilities, or can provide others of the above needed functions?
j. Is dissemination of NCIS analyses to new organizations needed?

To address and answer these questions adequately, consultation with other NCIS organizations is needed: LEPS, CTD, CID, and senior management. An affirmative answer to any one of them is an indication of the need to examine enhanced information exchange and collaboration capabilities, and how ASOCC and other systems can meet such requirements.

NCIS has put considerable effort into developing the Tactical Anti-Terrorism Information and Planning System (TATIPS). This was not a system to be fielded but a prototype for future development. It was used to determine web-based information system requirements for shipboard AT/FP planning in collaboration with MTAC, NCIS Field Agents, and their Fleet or Squadron. The system solved the bandwidth and connectivity problem by using the existing Collaboration at Sea system.

Other systems are either here or on the horizon. JRAMP is being instituted by CINCEUR for AT/FP planning, to be used by any unit coming into their theater. This means that MTAC and Navy ships may need to communicate around that system. IWCCS is a current Carrier Battle Group information system that is being brought ashore. It has situation awareness capabilities, such as sensor information display, is a candidate for some ASOCC-like functions, and is already in use by the Navy.

Collaboration between MTAC and operational ships is needed for AT/FP planning. IF real-time, rapid communications are needed, current systems are not adequate. Closest to real-time capability to all ships is provided by Collaboration at Sea. As noted above, TATIPS was developed to reside on this system. Unfortunately, an operational test of this capability has not been conducted. CONOPS and TTPs have not been developed for implementing such a real-time capability.

A comprehensive study is needed of the full spectrum of NCIS information and communication requirements, system requirements to support NCIS, and existing and planned systems. This would not be an overly arduous task. Such a study would lead directly to development of NCIS CONOPS and TTPs.

Appendix-1. COMPLETED ASOCC EVALUATION SURVEYS

ASOCC DEMONSTRATION - MTAC PARTICIPANT SURVEY

The following are your opinions. Base them on your personal experience in performing your job and on how ASOCC could contribute to that mission.

Name: ENS Erick Westlin Position: MTAC Analyst

A. Effort to perform a task with ASOCC compared to existing means.
Indicate the relative effort using the following scale

ASOCC is 1. much harder 2. harder 3. same 4. easier 5. much easier.

Provide these evaluations for the following functions, plus any other you wish to include.

1. Obtaining Information..... Ease _3_ Speed ___
2. Information dissemination..... Ease _2_ Speed ___
3. Collaboration with Law Enforcement..... Ease _4_ Speed ___
4. Collaboration with other agencies..... Ease _3_ Speed ___
5. Assessments ..... Quality ___ Ease ___ Speed ___

B. ASOCC System Performance

1. Ease of Navigation Hard ___ OK _X_ Easy ___

Describe any particular Navigation

Strengths

- Easy of use with little training enable easy navigation

Weaknesses

- sometimes the system would create a lock file, the user would not know if they were getting the most current information on X-Panel

2. System Design

Visual layout Poor ___ OK ___ Good _X_

Comments:

- 3 screens on this system does enable a lot more information to be seen at any given time.

Information comprehension Hard ___ OK _X_ Easy ___

Comments:

3. Desired Additional Capabilities: Describe

- the ability to communicate to more entities on the SIPRNET side. Most the information that NCIS MTAC is looking for or will need to pass is classified.

4. Design Strengths: Describe any components of system design you feel are particularly good.

- the collaboration element was a nice, real-time way of communicating with more than 1 person/agency/watch center. It enables the information to be passed or discussed between multiple parties.

5. Information Completeness: Is all the information you need there? Yes _X_ No ___
If no, describe what is missing.

C. Information Overload

Could you keep up with information you needed to review? Yes ___No_X_If no, describe:
Information desired:
-There could be information overload on the X-Panel.

Situation:
- When more than 1 ALERT comes across, the watch stander will not be able to tell where the alert came from in a time efficient way. There should be some sort of indicator in the ALERT window, stating who put the ALERT in. Maybe, if it was set up so that when you click a button in the ALERT window, it would take you to the logged event in X-Panel.

If no, would additional personnel solve the problem? Yes ___ No _X___How many? ____

D. Collaboration

Which collaboration capabilities did you use? Chat _X_ White Board _X___None ___

Ease of use	Hard	OK	Easy
Chat	___	___	_X_
White Board	___	___	_X_

Quality of Information	Good	OK	Poor
Chat	_X_	___	___
White Board	_X_	___	___

Comments:
- This tool is the most interesting of the tools for NCIS MTAC. We talk, gather, share information though out the community, and this tool allows MTAC to do that effectively.

E. New Capabilities

1. Does ASOCC allow new, useful activities to be performed? Yes ___ No _X_
If yes, Describe.

2. Does ASOCC provide useful information not normally available? Yes ___ No _X_
If yes, Describe.

F. Manpower

Is additional manpower needed in order to use ASOCC effectively? Yes ___ No_X_
For what functions?

If additional manpower were devoted to ASOCC use, would this be an efficient use of personnel for the MTAC operation? Yes ___ No _X_
Explain:
- At the current time, MTAC is undermanned. The MTAC Watch would be trained on this system, and use it as yet another tool to monitor information. The MTAC Watch could handle

this additional responsibility.

G. Situation Awareness
ASOCC's main purpose is Situation Awareness during a terrorist incident.
Is maintaining Incident Situation Awareness of use for MTAC operations? Yes _X__No ___
If yes, describe:
Situation within the event for which ASOCC information is useful:
- ongoing updates to a situation, casualties, nationality, Military Branch effected.

The information that would be useful:
- location of incident
- casualties
- who the incident affects

How the information would be used:
- MTAC would use information and updated information to produce SAR'S, SPOT reports, and/or BLUE Dart reports.

H. Special Interest Topics
There may be one of more topics you would like to especially convey about this system. If so, please describe here. Please number individual comments.

1) Once this system is fully operational, it would enhance the MTAC's capabilities. But, until this system the NCIS field offices and resident offices, ASOCC will not be very useful, other than monitoring for Law Enforcement information on the UNCLASSIFIED (NIPRNET).

2) The Collaboration tool was very interesting. I can see this enhancing the MTAC capabilities when more intel agencies join the system.

3) Disseminating information that the MTAC would put out via ASOCC does not reach the required assets that MTAC needs to reach (ie. naval ships) since they only have a very limited bandwidth to receive information.

4) Overall, I thought the experience with ASOCC very informative. The system possess the capability to enhance the situational awareness of the MTAC.

ASOCC DEMONSTRATION - Field Agent PARTICIPANT SURVEY

The following are your opinions. Base them on your personal experience in performing you job and on how ASOCC could contribute to that mission.

Name: Warren Brownley
Position: Special Agent, NCIS, Law Enforcement Liaison Officer,
Commander Navy Region Mid-Atlantic, Norfolk, VA

A. Effort to perform a task with ASOCC compared to existing means.
Indicate the relative effort using the following scale

ASOCC is 1. much harder 2. harder 3. same 4. easier 5. much easier.

Provide these evaluations for the following functions, plus any other you wish to include.

1. Obtaining Information..... Ease 5 Speed 5
2. Information dissemination..... Ease 5 Speed 5
3. Collaboration with Law Enforcement..... Ease 4 Speed 4
4. Collaboration with other agencies..... Ease 4 Speed 4
5. Assessments .....Quality 4 Ease 4 Speed 4

B. ASOCC System Performance

1. Ease of Navigation Hard ___ OK _ Easy X

Describe any particular Navigation

Strengths: Properly trained personnel can work the myriad of hypertext and icons for time sensitive access to information.

Weaknesses

2. System Design

Visual layout Poor ___ OK X Good ___

Comments: To the uneducated, the design is overwhelming at first but then becomes less complex with appropriate training and actual usage by the operator. It appeared that at least one screen at any given time was not being utilized, but that is an informational issue and not operator-related.

Information comprehension Hard ___ OK X Easy ___

Comments: As described above, at times it appeared that an overwhelming amount of information was bombarding the operator until that individual became familiar with ALL the info being projected. The amount of info available should be covered by at lease two if not three operators during the crisis management phase of the event.

3. Desired Additional Capabilities: Possibly two screens operated directly in front of two operators with an additional screen being used for imagery or on-scene, real time digital or analog video recording of the events taking place.

4. Design Strengths: Describe any components of system design you feel are particularly good. Strongest design feature was the running chat/commentary of the info readily available which was located on main screen for quick, easy read by decision-makers.

5. Information Completeness: Is all the information you need there? Yes X No ___

If no, describe what is missing.

C. Information Overload

Could you keep up with information you needed to review? Yes ____ No X If no, describe:

Information desired: There was a preponderance of information on the screens so no problem with the with the amount, but a problem with the most critical info that needs to be addressed by decision-makers. Recommendation: RED BLINKING LETTERING on info that is critical and needs immediate attention such as the discovery of a secondary device or event that effects the responders/rescue personnel.

Situation: At certain critical periods, information overload made it difficult for the laymen to discern what info was critical and what info was overcome by events (OBE).

If no, would additional personnel solve the problem? Yes X No ___
How many? At least one additional person to watch for critical, expedient info that the decision-makers need to know and evaluate while the other operators continue to monitor, analyze, and populate the databases/white board.

D. Collaboration

Which collaboration capabilities did you use? Chat ___ White Board ___ None ___

Ease of use	Hard	OK	Easy
Chat	___		X
White Board	___	___	X

Quality of Information	Good	OK	Poor
Chat	X	___	___
White Board	X	___	___

Comments: The use of the Personal Digital Assistant (PDA) to directly communicate to the command post or operations center alleviates the problem of no phone connection, hand-held radio inadequacy, media tying up all available emergency lines, to create real time comms to the incident commanders.

This system would have been beneficial to assist the LEAs during the Sniper Crisis by having one centrally located system with the perimeters, jurisdictions, crime scenes, responders' locations and other variables for the incident commanders to use for uniformity and efficiency.

E. New Capabilities

1. Does ASOCC allow new, useful activities to be performed? Yes X No ___

If yes, Describe: It allows the responders to forward real time information to the command posts and incident commanders for more expedient decision-making in the crisis and consequence mgt phases.

2. Does ASOCC provide useful information not normally available? Yes X No ___

If yes, Describe: It allows for real time data via the PDA to be forwarded to the screen, vice second/third hand info over telephone or radio lines which will become obsolete if power grids, telephone sites, or other comms lines are down.

F. Manpower

Is additional manpower needed in order to use ASOCC effectively? Yes X No___
For what functions? Analysts conducting Analysis, analysis, analysis of all the activity on each screen. The wealth of information becomes mute if there is no ongoing analysis that refines and bulletizes the most pertinent actions and locations for the incident commanders/decision-makers to grasp as soon as possible.

If additional manpower were devoted to ASOCC use, would this be an efficient use of personnel for the MTAC operation? Yes ___ No ___ N/A

Explain: Reporting agent was located at the field demonstration.

G. Situation Awareness

ASOCC's main purpose is Situation Awareness during a terrorist incident.
Is maintaining Incident Situation Awareness of use for MTAC operations? Yes ___ No ___
N/A; reporting agent was located at the field demonstration.

H. Special Interest Topics

There may be one of more topics you would like to especially convey about this system. If so, please describe here. Please number individual comments.

1) The law enforcement personnel (to include Naval Criminal Investigative Service) working the system need to have a strong analytical background combined with strong computer/technical skills. The ideal candidate to operate is a full-time analyst (ideally two analysts at the field office level) from the field office or headquarters level who has:

- Strong working knowledge of the field office's physical area of responsibility (AOR)
- Strong working knowledge of state and local LE / Fire Emergency agencies in the AOR
- 2-4 years experience as a dispatcher at the field office or other LE/emergency agency
- Technical skills to maintain operations in case of minor glitches, power outages, emergency situations

2) Ideally three special agents and one supervisory special agent assigned to the field office Crisis Response Team (or Major Crime Response Team) should receive training in the field aspects of using these collaborative tools in order to have at least one agent in the office at all times who can work the PDA to Chat / White Board system. Those agents should first receive training in areas of:

- Basic WMD Crisis Mgt / Disaster response training (field agents)
- Basic Incident Command System (supervisor) training
- Strong working knowledge of the ASOCC system to include exercise and real world experience in utilizing the system (in case of limited number of analysts and agents)
- Strong working knowledge of FBI Crisis Response system to ensure preservation of crime scene, setting perimeters, nomenclature used in crisis management phase

Appendix-2. MASTER SCRIPT INTRODUCTION

Following is the table of contents and the introduction to the ASOCC demonstration master script. It provides an understanding of the purpose and general structure of the demonstration. The full script is long and its inclusion here would add no additional understanding.

Master Script
Homeland Security C2 ACTD
December 2002 Demonstration

Introduction
I. Operational Participants
II. Scenario
III. Demonstration Design Methodology
Demonstration
Day One
Introductory Briefing
Indications and Warnings Phase
I. Washington D.C.
Part 1. Intelligence Summary
Part 2. Threat Advisories
II. Virginia: 1035 – 1050 EST
Part 1. Briefing
Part 2. Intelligence advisories from Norfolk and Chesapeake
III. Louisiana 1050-1110 EST
Part 1 - Briefing
Part 2 – Joint Intelligence Assessment
IV. Washington State – 1110 - 1125 EST
Part 1. Briefing
Part 3. Briefing
Break: 1125 – 1145 EST
Deterrence, Prevention and Protection Phase
V. Washington, D.C. 1145-1150 EST
Part 1. Intelligence Summary
Part 2. Advisories
VI. NORTHCOM Preparations
A. Maritime Defense – 1150 - 1215 EST
Part 2 – Advisories
Part 3. Assessment of Ship with Nuclear Weapon aboard
Part 4. XIS track file demonstration
B. MACA – 1215-1220 EST
VII. Navy and Marine Washington Ops Centers – 1220-1225 EST
VIII. Hampton Roads
A. Navy – 1225-1235 EST
B. Virginia Local Federal, State and Local – 1235 - 1245 EST
IX. Louisiana 1245 – 1300 EST
Lunch Break 1300-1345 EST
Deterrence, Prevention and Protection Phase – Part 2
X. California – 1345 - 1355 EST
XI. Washington State – 1355 - 1410 EST
XII. New York – 1410-1420
Break – 1420 – 1435 EST
XIII. NORTHCOM Maritime Defense – Success – 1435 - 1440 EST
Louisiana Barge Tow Explosion Part 1
XIV. DTRA briefing of Explosion – 1440 - 1445 EST

XV. Initial Response – 1445 - 1505 EST
The demonstration is concluded for today
1515 EST – Louisiana Event 62 rehearsal
1600 EST – Navy / Marine Corps Washington Area and West Coast rehearsal
Day Two
Louisiana Barge Tow Explosion Part 2
XVI. Crisis Action Planning – 1000 – 1045 EST
Break – 1045-1100 EST
XVII. Crisis and Consequence Management 1100-1145 EST
Break – 1145-1200 EST
Terrorist Attacks and Crisis Action Planning - Hampton Roads and San Diego
XVIII. DTRA Briefing of Attacks 1200-1210 EST
XIX. Initial Response
A. Washington, D.C. – 1210 - 1215 EST
B. Hampton Roads
1. Navy – 1215 - 1230 EST
2. Local Federal agencies, State and Local governments 1230-1245 EST
Lunch Break – 1245-1330 EST
Preparations for Events 110 and 111
Terrorist Attacks - Hampton Roads and San Diego – Continued
XX. Crisis Action Planning Phase
A. Washington D.C. – 1330 - 1345 EST
B. Hampton Roads
1. JTF-CS – 1345-1400 EST
2. Navy – 1400-1405 EST
3. Virginia – Local Federal, State and Local – 1405-1430 EST
C. New York – 1430-1445 EST
Break 1445-1500 EST
Preparations for events 113 – 123 and 132-134
D. California 1500 - 1550 EST
1. Attack Phase
2. Crisis Action Planning Phase
E. New York
Break 1550-1600 EST
XXI. Crisis and Consequence Management Phase
A. Hampton Roads 1600-1645 EST
1. Navy
2. Virginia Local Federal, State and Local
B. California

Introduction

Operational Participants

This script is written in support of a technology demonstration in December 2002 sponsored by DoD's Homeland Security Command and Control [C2] Advanced Concept Technology Demonstration [ACTD]. Participants in the operations supported by the technologies and

concepts of operations in this demonstration include:
I. Within DOD, the Northern Command, the Navy and Marine Corps, DIA's Joint Intelligence Task Force – Counterterrorism [JITF-CT], DISA, NRL and DTRA;
II. Key elements of the Federal Law Enforcement community including the FBI, ATF, Marshals Service, Coast Guard and the Naval Criminal Investigative Service [NCIS] Multiple Threat Analysis Center [MTAC];
III. The National Intelligence Community including CIA, NSA and NIMA [plus DIA mentioned above];
IV. The Office of Homeland Security;
V. other federal agencies;
VI. Three states [Virginia, Louisiana, and Washington] including participation by State EOCs, State Police, and National Guard;
VII. Three cities [New York, Norfolk and Chesapeake] including EOCs, Fire and Rescue and Police Departments;
VIII. A county government [Pierce County in Washington State]; and

Participants will be located in Tacoma, San Diego, Colorado Springs, Baton Rouge, Hampton Roads, the Washington D.C. area and New York City.

Scenario

The scenario is designed to support demonstrations of concepts of operations and technology support to every participating organization and echelon, including:
IX. Management of and collaboration between echelons within single organizations
X. Collaboration among federal, state and local organizations at every echelon from federal agencies in Washington D.C. and State EOCs to city/county EOCs to responders at incident scenes including federal, state and local law enforcement personnel and fire fighters.

Within the demonstration scenario, the national intelligence community will develop information and assessments that Al Qaeda has obtained weapons of mass destruction and is shipping them to the U.S. on merchant ships. The intelligence will then be developed to the point that the Navy [NAVNORTH] is able to intercept and neutralize the ships under the direction of NORTHCOM in a homeland defense [HLD] mission.

While the Navy and Coast Guard are working to intercept the ships, there is a suspicious explosion on the Mississippi river near an oil refinery facility in Baton Rouge. State and local authorities led by the Louisiana State Police and federal law enforcement organizations led by the Coast Guard investigate with the analytical assistance of DoD [DTRA]. State and local law enforcement and consequence management authorities and the Coast Guard coordinate with federal law enforcement and intelligence agencies in assessing the explosion for links to terrorism.

As the investigation in Louisiana is nearing completion, terrorist cells in Hampton Roads and in San Diego execute suicide attacks coordinated to occur simultaneously in both locations. Car and truck bomb attacks are successful at in Hampton Roads Virginia at NS Norfolk, Norfolk International Terminals, the Berkley Bridge in Norfolk, "Tidewater Energy" in Chesapeake and MCAS Miramar in San Diego.

XI. In Hampton Roads, the blasts and associated hazardous chemicals cause major damage, deaths and injuries and result in some panic and mass evacuations. Multiple incident sites in Hampton Roads require coordination among the Norfolk Naval Station, the city of Norfolk and the city of Chesapeake and among the unified commands at the incident scenes.
XII. In San Diego, the attacks at Miramar kill gate personnel, shut down the base and require extensive HAZMAT cleanup. The defensive sensor arrays at NAS North Island, cued by intelligence, detect a suicide speedboat attack enabling defensive forces defeat it.

These situations require extensive federal, state and local crisis and consequence management efforts including military assistance to civil authorities [MACA] in Hampton Roads as well as Navy and Marine antiterrorism/force protection [AT/FP] measures at NS Norfolk and MCAS Miramar. NORTHCOM MACA and Navy AT/FP efforts in Hampton Roads are coordinated within the military, and all military efforts in Hampton Roads and San Diego are coordinated with federal, state and local authorities.

Demonstration Design Methodology

Participants in the demonstration have designed and scripted their own roles, thus ensuring that demonstration is relevant to each of them. Information technology is employed in the demonstration to provide visualization and decision support at every echelon and to support and manage online information flows and collaboration:
XIII. In alerting, deterrence, prevention and protection phases, from Washington to the states and localities and, once alerted, from localities back up to the state and federal governments
XIV. In the aftermath of the attacks, among unified commands of federal, state and local responders at incident scenes, from incident scenes to local civilian and military EOCs, among the EOCs themselves and from the EOCs to the state capitals, military commanders and Washington.

For purposes of the demonstration, we will open up all information within the demonstration to all participants in the demonstration on the networks to which they have subscribed. In other words, demonstration sites all over the nation participating in the unclassified DCTS network will be able to hear [audio teleconference] and see [on ASOCC and/or browser/NetMeeting screens] the demonstration vignettes in Hampton Roads, Louisiana and the other venues. Similarly, participants in the SIPRNET network will be able to hear the audio conference and see SIPRNET activities. This is an artificiality of the demonstration. For operational deployments of ASOCC and DCTS, appropriate server suites and access controls will be instituted for day-to-day use of the organization or affinity group that sponsors the deployment. Examples of affinity groups might include groups of base and city emergency services agencies in a region such as Hampton Roads; groups of law enforcement agencies; groups of state agencies; etc. Even within an organization or affinity groups, access to specific information such as law enforcement data may be subject to additional controls. In actual operations, the design and integration of DCTS and ASOCC will permit users to grant temporary access to those outside established affinity groups with a need to know, and especially those with a need to collaborate.

Appendix-3. NETWORK BASED INFORMATION SYSTEM REQUIREMENTS

The following are the requirements that were developed for the Tactical Anti-Terrorism Information and Planning System (TATIPS). This system was designed to support collaborative interaction between, MTAC, NCIS Field Agents, and Navy ships during AT/FP planning.

The complete information system is to include the network based system, e-mail, message traffic, and standard VTC and phone communications. This section describes only the network based system configuration.

Entry Point and Browsing

Entry to the system will normally be through the Operational Unit home page, such as that of Third Fleet. That page will have a link to the AT/FP home page.

Then AT/FP home page will have links to

- Agency Home Pages,
- Intelligence Information Reports (IIR) Page,
- Requests For Information (RFI) Page, and most importantly
- specific Operation Page.

This page will have a permanent URL, so that one can go to it directly.

The Operation Page contains links to all information that is pertinent to a *specific operation.* There is a page for each operation that is currently underway. There will be links to:

- Participant Information
- Threat Assessment
- Political Assessment
- Host Nation Support
- IIRs
- RFIs
- AT/FP Plans
- Logistics Requests
- Bulletin Board
- Chat Room

This page will have a permanent URL, so that one can go to it directly.

The following describes each of these pages and the logic behind the paths.

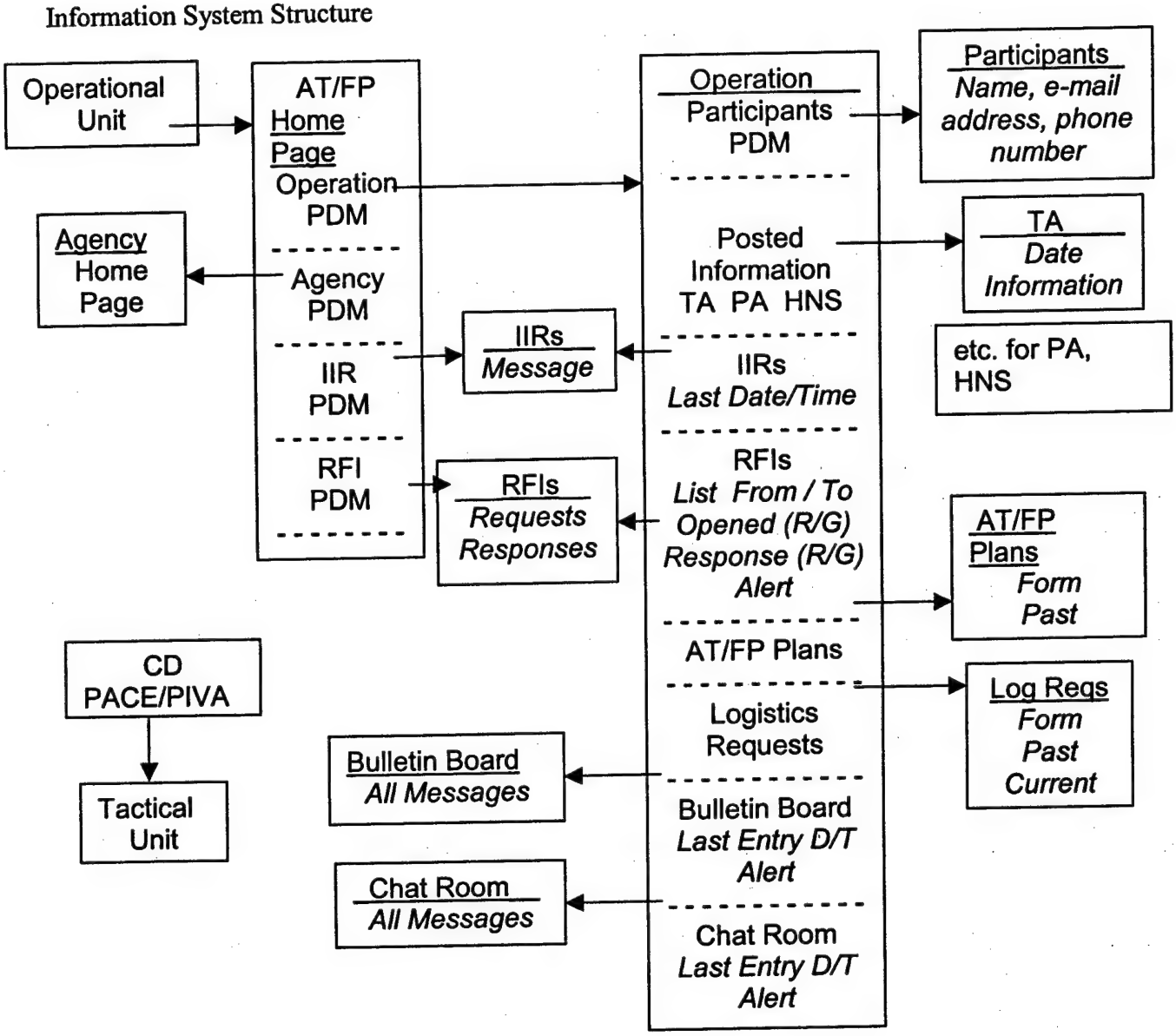
Operation Page Creation

The Operation Page is the hub of the information system. It is created by the NCIS Multi-Threat Alert Center (MTAC). They open a Page on request or when informed that an operation will occur that requires AT planning. Separate Pages will exist for each operation.

MTAC will populate the Page with information they have in their "drawers" and reach out to other agencies for pertinent information they have available. MTAC will operate as the information filter and fuser. They have control of the initial information that populates the site.

After the initial population has occurred, participants in the operation can post and request information without going through MTAC. An process will be needed to authorize participants for an operation, but this is not an implementation requirement for initial site development.

Information System Structure



Each box is a web page, with the page title underlined at the top. Each page contains areas, which are separated by dashed lines and titled. The information contained within each page or area is indicated by italics.

An arrow originating within a box indicates a link from that box to the page shown. PDM means that there is a pull down menu within that area to provide links to the page shown.

Note that 3 is the maximum number of mouse clicks from one place to another in this scheme.

Content Descriptions

Operational Unit Page: This page is the first entry point into the system. It is the home page of the organization that has cognizance over the operation, e.g. Fleet, Region. A link is needed to the AT/FP home page. It is uncertain at this time whether there will be a separate AT/FP page for each operational unit or whether there will be a universal page.

AT/FP Home Page: This is the central hub for stepping to any desired AT/FP information.

Operation PDM: Each operation will have a name that easily identifies it to the user. The pull down menu will be used to access the specific operation of interest.

Agency PDM: The pull down menu allows the user to go to a specific agencies home page for either information or communication.

IIR PDM: One would normally be interested in IIRs for a specific operation and access them through the Operation page. This link is present to allow one direct access to IIRs. However, the access is through a PDM, which is operation names, so one has to step back and forth to access IIRs for more than one operation.

RFI PDM: The philosophy and structure is the same as for IIRs.

Archives: The requirements for archive structure have not yet been developed. An archive of some sort is needed, with the structure defined by potential users.

Operation Home Page: There is a separate page for each operation. Only information for the specific operation can be accessed from this page.

Participants PDM: The PDM contains the name and organization of each approved participant and a link to their information.

Posted Information: Direct links to Threat Assessments, Political Assessments, and Host Nation Support pages are provided.

IIRs: A direct link to the IIR page is provided. Also shown is the date/time of the last IIR.

RFIs: A direct link to the RFI page is provided. Also shown through a PDM is the name for each request, whom it is from and to, whether it has been opened, and whether a response has been generated. An alert is shown for outstanding requests.

AT/FP Plans: A direct link to the AT/FP page is provided.

Logistics Requests: A direct link to the Logistics Request page is provided.

Bulletin Board: A direct link to the bulletin board page is provided. Also shown is the date/time of the last entry. An alert is shown for entries for which a response is requested.

Chat Room: A direct link to the bulletin board page is provided. Also shown is the date/time of the last entry. An alert is shown for entries for which a response is requested.

Participants: This is a list of all persons given access to this operation's information. It contains their e-mail address and phone number so they can be contacted directly.

Threat Assessments (TA): All TAs that are deemed germane to this operation are posted on this page. Each TA is accompanied by the date it was issued so its currency can be determined.

Political Assessments (PA): All PAs that are deemed germane to this operation are posted on this page. Each PA is accompanied by the date it was issued so its currency can be determined.

Host Nation Support (HNS): HNS is a stable support environment in many situations, but can change rapidly in others. Thus, this page will sometimes contain several HNS documents. The documents will be time ordered with the time of issue indicated. See the alerting description later in this section.

AT/FP Plans: AT/FP plans are required for various operational situations. This page will contain the form that is to be submitted for the particular operation. It will also contain examples of forms that have been completed and submitted for similar operations or, preferably, for that same location. The current, active plan for this operation is present. If there has been more than one plan submitted, the original plan and the current update are present. *Note: depending on the C2 process for the operation, it may be necessary to have ISIC approval before a plan can be posted on this page.*

Logistics Requests: Logistics Requests are required for various operational situations. This page will contain the form that is to be submitted for the particular operation. It will also contain examples of forms that have been completed and submitted for similar operations or, preferably, for that same location. The current, active request for this operation is present. If there has been more than one request submitted, the original request and the current update are present. *Note: depending on the C2 process for the operation, it may be necessary to have ISIC approval before arequest can be posted on this page.*

Intelligence Information Reports (IIRs): This page contains all IIRs that have been transmitted for the operation, in time order. See the alerting description later in this section.

Requests for Information (RFIs): This page contains all RFIs requests and responses that have been transmitted for the operation, in time order of the request. A given request and response are collocated. See the alerting description later in this section.

Bulletin Board: This is a standard bulletin board. The system must have the capability to archive, store, and make available the information at the end of each day and operation. See the alerting description later in this section.

Chat Room: This is a standard chat room. The system must have the capability to archive, store, and make available the information at the end of each day and operation. See the alerting description later in this section.

PACE/PIVA CD: PACE and PIVA are being combined into a single product for AT/FP use. PACE is too large for many platforms to be able to access through the internet, and the same will be true for the combined product. Thus, CDs will be burned with the information and provided to units. This programs information system may provide updates to that information.

Multi-Path Information

Some information must go directly to tactical and operational units. They may not have current access to the web or may not be standing a "web watch". Thus, some information must go directly to them as well as being posted on the web. This applies to

RFIs
IIRs
TA updates

HNS updates will be provided to the tactical unit locally.

Quite useful would be to place information on the web and have that occurrence generate the message that goes direct point-to-point. It is unknown whether such a capability can be developed.

Alerting

Various pieces of information are time critical and an alerting system is needed to insure they are seen and/or timely action is taken. Following are those information for which alerts are needed and the type of alert.

AT/FP plan - due date.
Logistics Request - due date.
Bulletin Board - alert recipient of an items presence when desired by the person posting.
Chat - alert recipient of an items presence when desired by the person posting.
IIR- alert affected operational and tactical units and local agents.
RFI - alert request recipient, alert requestor when a response is sent.

Besides the direct alerts, the information system should show the status of information. Desired status information is listed in the previous material describing information on the web pages.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center 8725 John J. Kingman Rd., STE 0944 Ft. Belvoir, VA 22060-6218	2
2.	Dudley Knox Library, Code 013 Naval Postgraduate School Monterey, CA 93943-5100	2
3.	Research Office, Code 09 Naval Postgraduate School Monterey, CA 93943-5138	1
4.	Mike Stumborg Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
5.	Mike Dorsey Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
6.	LCDR Tim Tutt Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
7.	LTJG Eric Westlin Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
8.	Bill VonStorch Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
9.	Special Agent Cliff Link Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1

10.	Agent Warren Brownley, N2 Commander Navy Region Mid-Atlantic 6506 Hampton Blvd. Norfolk, VA 23508-1273	1
11.	Gordon Schacher Wayne Meyer Institute of Systems Engineering Naval Postgraduate School 777 Dyer Rd., Rm 100D Monterey, CA 93943	2
12.	Shelley Gallup Wayne Meyer Institute of Systems Engineering Naval Postgraduate School 777 Dyer Rd., Rm 100D Monterey, CA 93943	5